Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-6, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Data Confidentiality in Cloud Computing Using Android Application

Shital S. Jadhav, Priya K. Hagwane,
Priyanka C. Labhade & Kavita S. Nalawde
Guided By: Prof. Kunal Ahire
(Department Of Information Technology, MET's Institute Of Engineering,Adgaon, Nashik)

Abstract: *Cloud Computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud soas to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in Cloud Computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. The key feature of out project is,we also try to achieve the convenience for usage of our idea we create An Android application which is easy to access and use . In this there is single user_id for single mobile which is unique IMEI(International Mobile station Equipment Identity) number of each mobile of user so that security issue is solved. Thus, also enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective Third Party Auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The Third Party Auditing process should bring in no new vulnerabilities towards user data privacy. In this paper we are extending the previous system by using automatic blocker for privacy preserving public auditing for data storage security in cloud computing. we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique and automatic blocker. to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient with mobility feature.*

Keywords:
CC : Cloud Computing
TPA : Third Party Authentication
PB : Protocol Blocker
CSP : Cloud Service Provider
IMEI : International Mobile Station Equipment Identity

Introduction

Cloud Computing has been envisioned as the next-generation architecture of IT enterprise, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk [1]. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced into the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely into the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc [2].While these advantages of using clouds are unarguable, due to the opaqueness of the Cloud—as separate administrative entities, the internal operation details of Cloud Service Providers (CSP) may not be known by cloud users—data outsourcing is also relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity. Examples of outages and security breaches of noteworthy cloud services appear from time to time [3–6]. Secondly, for the benefits of their own, there do exist various motivations for cloud service providers to behave unfaithfully towards the cloud users regarding the status of their outsourced data In short, although outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. Recently, the notion of public auditability has been proposed in the context of ensuring remotely stored data integrity under different systems and security models [7, 9]. Public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes [7, 9,] do not support the privacy protection of users' data against external auditors, i.e., they may potentially reveal user data information to the auditors, From the perspective of protecting data privacy, the users, who own the data and rely on TPA just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage towards their data security. Exploiting data encryption before outsourcing is one way to mitigate this privacy concern, but it is only complementary to the privacy-preserving public auditing scheme to be proposed in this paper. Thus, it does not completely solve the problem of protecting data privacy but just reduces it to the one of managing the encryption keys. Here by following the aspects and we are using automatic blocker to the cloud environment, which particularly blocks the auditing protocols from unauthorized access from the external user for privacy preserving for data security in cloud computing.

II. Related Work

Ateniese et al. [7] are the first to consider public auditability in their defined "Provable Data Possession" (PDP) model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA-based homomorphic authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. .When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. Juels et al, describe a "Proof of Retrievability" (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is a fixed priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Shacham et al, design an improved PoR scheme built from BLS signatures with full proofs of security in the security model defined in. Similar to the construction in [7], they use publicly verifiable homomorphic authenticators that are built from provably secure BLS signatures. Based on the elegant BLS construction, public retrievability is achieved. Again, their approach does not support privacy-preserving auditing for the same reason as [7]. Shah et al. [8], propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies both the integrity of the data file and theserver's possession of a previously committed decryption key.

This scheme only works for encrypted files, and it suffers from the auditor statefulness and bounded usage, which may potentially bring in on-line burden to users when the keyed hashes are used up. In other related work, Ateniese et al. propose a partially dynamic version of the prior PDP scheme that uses only symmetric key cryptography[a]. However, all their protocol requires the linear combination of sampled blocks just as [7], and thus does not support privacy-preserving auditing on user's outsourced data. Previous systems proposed that A public auditing scheme consists of four algorithms (Keyed, SigGen, GenProof, VerifyProof). KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification metadata, which may consist of MAC, signatures, or other related information that will be used for auditing. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof from the cloud server. Public auditing system can be constructed from the auditing scheme in two phases, Setup and Audit[a], The previous system starts with with two warmup schemes. The first one does not ensure privacy-preserving guarantee and is not as lightweight as we would like. The second one overcomes the first one, but suffers from other undesirable systematic demerits for public auditing: bounded usage and auditor statefulness, which may pose additional on-line burden to users as will be elaborated shortly. We believe the analysis of these basic schemes will leadus to our main result, which overcomes all these drawbacks. Basic Scheme I and Basic Scheme II [a]. The Privacy-Preserving Public Auditing Scheme[a], Batch Auditing[a], Data Dynamics [a].Our proposed system enable privacy-preserving public auditing for cloud data storage under the aforementioned model, our protocol.

design should achieve the following security and performance guarantee:

1. Public Auditability
to allow TPA to verify the correctness of the cloud data on demand without retrieving a copy of the whole data or introducing additional on-line burden to the cloud users.

2. Storage Correctness
to ensure that there exists no cheating cloud server that can pass the audit from TPA without indeed storing users' data intact.

3. Privacy-Preserving
to ensure that there exists no way for TPA to derive users' data content from the information collected during the auditing process;

4. Batch Auditing
to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously.

5. Lightweight
to allow TPA to perform auditing with minimum communication and computation overhead.

III. Proposed System

We start from the overview of our system. we adopt the automatic blocker at the cloud server, whenever a unauthorized user access the users data from cloud storage, the system runs an tiny application to monitor the user inputs, it matches to give access otherwise does not give user access by blocking the protocols.

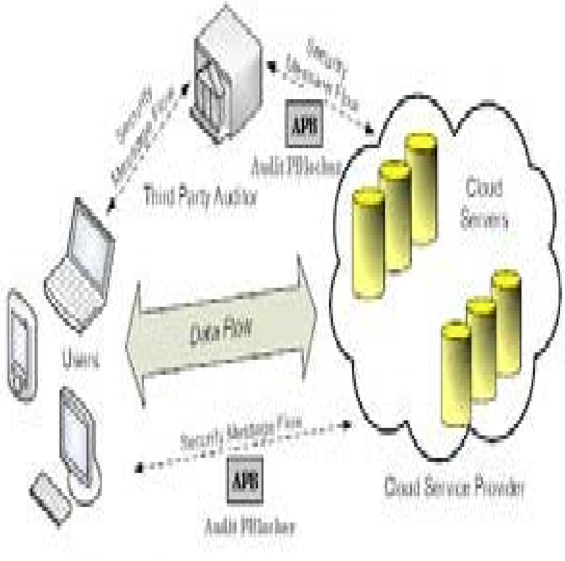

Fig. 1: The architecture of cloud data storage service

Our work is among the first few ones to support privacy-preserving public auditing in Cloud Computing, with a focus on data storage. The System and Threat Model: We consider a cloud data storage

1. the cloud user (U), who has large amount of data files to be stored service involving three different entities in the cloud;

2. the Cloud Server (CS), which is managed by Cloud Service Provider (CSP) to provide data storage service and has significant storage space and computation resources

3. Audit Protocal Blocker (APB) The proposed system incorporates the previous system advantages and extends to find the unauthorized user,to prevent the unauthorized data access for preserving data integrity. The proposed system monitors the user requests according the user specified parameters and it checks the parameters for the new and existing users .The system accepts existing validated user, and prompts for the new users for the parameter to match requirement specified during user creation for new users. If the new user prompt parameter matches with cloud server, it gives privileges to access the Audit protocol authorwise the system automatically blocks the Audit protocol for specific user.

System Modules:
The propose System is Developed with extended vision for user's Simplicity. We create an Application which is supported by mostly Smartphones for Storage of the data efiiciently.
The Proposed system having 4 Different Modules:
1.Registration
2.Login
3.Storage Operations.
4.Atomatic Protocol Blocker.

1.Registration:
In this Module the User has to Install the Application on his/her android device and then by filling the necessary information like name, email_id ,contact number. The validation is also done in this phase if in case user place a wrong information system gives notification. The validation is necessary because the further OTP generation. In this phase the User Id is IMEI number of each cell phone which is Unique. The registration phase is sub divided into two parts:

A. OTP Generation
B. Setting 3D password

A.OTP Generation:

The OTP(The One-Time Password) system is a Two-Factor Authentication system where the password constantly alternates. This greatly reduces the risk of an unauthorized intruder gaining access to the account.

- The main benefit of OTPs is to prevent eavesdropping. Even if an attacker gets the temporary password he will only be able to use it during the time your session is opened.

- It avoids different types of attacks such as brute force attack, dictionary attack etc.
- It uses hash function for generation of password. The one-time password system works by starting with an initial seed *s*, then generating passwords

$$f(s), f(f(s)), f(f(f(s))), \ldots$$

as many times as necessary.

B. Setting 3D password :

- The idea is simply outlined as follows. The user navigates through a three dimensional virtual environment. The combination and the sequence of the user’s actions and interactions towards the objects in the three dimensional virtual environment constructs the user’s 3D password
- 3D Passwords are not easy to write down on paper. Passwords are difficult to crack .It provide large password space. It avoids brute force attack, dictionary attack,
- Thus we have conclude that the proposed system is multilevel authentication system which increases the level of security as compared to single authentication system.

2. Login

Once the registration has been completed the user has only enter the password while using the application just like to enter the pattern lock for unlocking keypad. The set password is nothing but only moving the moves of 3D chessboard which has been set at the time of registration.

3. Storage Operations.

The storage operation include the Uploading and Downloading of the file data which is in the file manager of the device. The data may be in image, pdf or text and any other format. User has to just click on the Add button of the screen then the files belongs to the file manager are display and from which user have to select the file for storing on the cloud. At the Server (Cloud) side the data is divided into ‘n’ number of chunks and this chunk store on the multi locations within cloud such that no one can get the data from single chunk. For retrieving the data the user must have to prove his/her authentication by setting password again. The chunks again gather together to form the real data file. The use of chunk is for avoiding attack because of single chunk attacker does not get sense about the data.

4. Automatic Protocol Blocker.

The proposed system incorporates the previous system advantages and extends to find the unauthorized user ,to prevent the unauthorized data access for preserving data integrity. The proposed system monitors the user requests according the user specified parameters and it checks the parameters for the new and existing users .The system accepts existing validated user, and prompts for the new users for the parameter to match requirement specified during user creation for new users. If the new user prompt parameter matches with cloud server, it gives privileges to access the Audit protocol authorwise the system automatically blocks the Audit protocol for specific users .Project Definition Outsourcing data into the cloud is economically attractive for the cost and complexity of long-term large-scale data storage, it does not occuer any guarantee on data integrity and availability.This problem, if not properly addressed, may impede the successful deployment of the cloud architecture. When the user stores his data on the cloud, there are so many chances of data loss. When user data is lost, at that time it is difficult to get his original data and identify what changes is done by the hacker. Sometime user can't understand what modification is done by the hacker.

Functional Requirements
Specification

The system is proposed to have the following modules:
_ Admin Module
_ TPA module
_ User module
_ Block Verification Module
_ Block Insertion Module
_ Block Deletion

Admin module:
Admin is allowed to check which user registered and which data is stored in the cloud space.

TPA Module:
TPA check that data is modified or not if modified that information send to user

User Module:
User can register and he can login with his user id and password and he can upload the data to cloud space area

Block Verification Module:
User can check that the uploaded file is modified by any one or not(like server area)

Block Insertion Module:
In the block insertion module user can insert the new block

Block Deletion Module:
In the Block Deletion Module user can delete the Block.

References

[1] IEEE INFOCOM 2010, San Diego, CA, March 2010.

[2] P. Mell, T. Grance (2009),“Draft NIST working definition of cloud computing”, [Online]Available: http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, M. Zaharia,“Above the clouds: A berkeley view of cloud computing”, University of California, Berkeley, Tech. Rep.UCB-EECS-2009-28, Feb 2009.

[4] N. Gohring (2008), “Amazon’s s3 down for several hours”,[OnlineAvailable: http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html

[5] Amazon.com (2008), “Amazon s3 availability event: [Online]Available:http://wwwstatus.aws.amazon.com/s3-20080720.html

[6] S. Wilson (2008), “Appengine outage”, [Online] Available: http://www.cio-weblog.com/50226711/appengine outage.php.

[7] B. Krebs,“Payment Processor Breach May Be Largest Ever”, [Online]Available:http://www.voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.

[8] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, D. Song,“Provable data possession at untrusted stores”, Cryptology ePrint Archive, Report 2007/202, 2007, [Online] Available: http://www.eprint.iacr.org/.

[9] M. A. Shah, R. Swaminathan, M. Baker,“Privacy-preserving audit and extraction of digital contents”, Cryptology ePrint Archive, Report 2008/186, 2008, [Online] Available: http:// www.eprint.iacr.org/.

[10] Q. Wang, C. Wang, J. Li, K. Ren, W. Lou (2009),“Enabling public verifiability and data dynamics for storage security in cloud computing”, in Proc. of ESORICS’09, Saint Malo,France.